Docket No.: 1080.1096/JDH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Yoshihiro NAKAGAWA

Group Art Unit: To Be Assigned

Serial No.: To Be Assigned

Examiner: To Be Assigned

Filed: April 18, 2001

For: INDIVIDUAL INFORMATION MANAGING DEVICE

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, Applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-397492 filed December 27, 2000.

It is respectfully requested that Applicants be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Dated: April 18, 2001

By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant(s): SUMIDA, Yoshiaki

Application No.: Group:

Filed: April 30, 2001 Examiner:

For: WIRELESS SEARCH DEVICE

L E T T E R

Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

April 30, 2001
1152-0276P

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55(a), the applicant hereby claims the right of priority based on the following application(s):

Country	Application No.	Filed
JAPAN	2000-228905	07/28/00

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. 1.16 or under 37 C.F.R. 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By: _____
CHARLES GORENSTEIN
Reg. No. 29,271
P. O. Box 747
Falls Church, Virginia 22040-0747

Attachment
(703) 205-8000
/pf

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年１２月２７日

出 願 番 号
Application Number: 特願２０００－３９７４９２

出 願 人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年 ３月１６日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３０１９４１９

【書類名】　特許願
【整理番号】　0090210
【提出日】　平成12年12月27日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明の名称】　個人情報管理装置
【請求項の数】　7
【発明者】
【住所又は居所】　香川県高松市錦町１丁目１１番１号　株式会社富士通四国インフォテック内
【氏名】　中川　喜博
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100094330
【弁理士】
【氏名又は名称】　山田　正紀
【選任した代理人】
【識別番号】　100109689
【弁理士】
【氏名又は名称】　三上　結
【手数料の表示】
【予納台帳番号】　017961
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【包括委任状番号】　9912909

【プルーフの要否】　　要

【書類名】　　明細書

【発明の名称】　個人情報管理装置

【特許請求の範囲】

【請求項１】　通信回線網に接続された、個人情報を管理する個人情報管理装置であって、

個人ごとの情報が登録された個人情報格納部と、

各個人により指定された各個人ごとの情報開示手続が登録された開示手続格納部と、

通信回線網を経由した、特定の個人の情報の開示依頼を受け、前記開示手続格納部に格納された、該特定の個人の情報開示手続に合致した情報開示手続を実行し、該情報開示手続が満足された場合に該特定の個人の情報を依頼元に向けて通信回線網に送信する開示手続実行部とを備えたことを特徴とする個人情報管理装置。

【請求項２】　前記個人情報格納部は、個人ごとの情報の中の各個別の情報それぞれが各個人により複数のランクのうちのいずれかのランクに指定されることにより、各個人内で複数にランク付けされてなる個人情報が登録されたものであり、

前記開示手続格納部は、各個人により指定された、各個人内の各ランクに応じた情報開示手続が登録されたものであって、

前記開示手続実行部は、特定の個人の情報の開示依頼を受け、前記開示手続格納部に格納された、該特定の個人の、開示依頼を受けた情報のランクに応じた情報開示手続に合致した情報開示手続を実行するものであることを特徴とする請求項１記載の個人情報管理装置。

【請求項３】　前記開示手続格納部は、各個人により指定された、各個人ごとの平常時の情報開示手続に加え、各個人により指定された、各個人ごとの緊急時の情報開示手続が登録されたものであって、

前記開示手続実行部は、平常時と緊急時とを識別する情報を伴った、特定の個人の情報の開示依頼を受け、該開示依頼が平常時あるいは緊急時のいずれに属するかに応じて、前記開示手続格納部に格納された、該特定の個人の、それぞれ平

常時の情報開示手続あるいは緊急時の情報開示手続に合致した情報開示手続を実行するものであることを特徴とする請求項１記載の個人情報管理装置。

【請求項４】　前記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、該各個人への連絡手続が登録されたものであって、

前記開示手続実行部は、特定の個人の情報の開示依頼を受けて、該特定の個人に、前記開示手続格納部に格納された該特定の個人への連絡手続に合致した連絡手続で、個人情報の開示依頼があった旨通知して、通知を受けた個人からの情報開示の承認を受ける開示依頼通知部を備え、該開示依頼通知部により情報開示の承認を受けて、さらに情報開示手続を進めるものであることを特徴とする請求項１記載の個人情報管理装置。

【請求項５】　前記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、該各個人本人であることを認証する認証手続が登録されたものであって、

前記開示手続実行部は、特定の個人の情報の開示依頼を受けて、前記開示手続格納部に格納された該特定の個人の認証手続に合致した認証手続で該特定の個人の認証を行なう認証部を備えたものであることを特徴とする請求項１記載の個人情報管理装置。

【請求項６】　前記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、該各個人本人であることを認証する認証手続が登録されたものであって、

前記開示手続実行部は、該特定の個人の前記開示依頼通知部により情報開示の承認を受けた後において、前記開示手続格納部に格納された前記特定の個人の認証手続に合致した認証手続で該特定の個人の認証を行なう認証部を備えたものであることを特徴とする請求項１記載の個人情報管理装置。

【請求項７】　前記開示手続格納部は、個人ごとに、該個人に代わって情報開示手続を進める権限が委譲された権限委譲者の登録が自在なものであって、

前記開示手続実行部は、特定の個人の情報の開示依頼を受け、前記開示手続格納部に該特定の個人に代わって情報開示手続を進める権限が委譲された権限委譲

者が登録されていた場合には、該特定の個人の情報を開示するための手続として、該開示手続格納部に格納された該権限委譲者の情報開示手続に合致した情報開示手続を実行するものであることを特徴とする請求項１記載の個人情報管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信回線網に接続された、個人情報を管理する個人情報管理装置に関する。

【０００２】

【従来の技術】

近年、パーソナルコンピュータどうしを接続するインターネットの利用率が急進しており、例えば医療現場においても、電子カルテシステムの運用にデータセンタが利用されインターネットを通じてアクセスされるなど、様々な分野において情報管理システムそのものが変わってきている。

【０００３】

【発明が解決しようとする課題】

このように急速に変化しつつある社会環境下において、例えば上記の電子カルテシステムにおける個人のカルテ情報などの個人情報がインターネットを介して不用意に開示あるいは公開されてしまうことを防止し、個人に不測の不利益を及ぼしかねない状況を生じさせないシステムを構築することが急務となってきている。

【０００４】

本発明は、上記事情に鑑み、個人情報の保護が図られた個人情報管理装置を提供することを目的とする。

【０００５】

【課題を解決するための手段】

上記目的を達成する本発明の個人情報管理装置は、通信回線網に接続された、個人情報を管理する個人情報管理装置であって、

個人ごとの情報が登録された個人情報格納部と、

各個人により指定された各個人ごとの情報開示手続が登録された開示手続格納部と、

通信回線網を経由した、特定の個人の情報の開示依頼を受け、開示手続格納部に格納された、その特定の個人の情報開示手続に合致した情報開示手続を実行し、その情報開示手続が満足された場合にその特定の個人の情報を依頼元に向けて通信回線網に送信する開示手続実行部とを備えたことを特徴とする。

【０００６】

本発明の個人情報管理装置は、各個人により指定された、各個人ごとの情報開示手続を格納しておいて、ある特定の個人の情報開示にあたっては、その特定の個人によりあらかじめ指定されている情報開示手続に従って情報開示を行なうものであり、その個人の意に反した情報開示は防止され、したがってその個人が不測の不利益を被ることが防止される。

【０００７】

ここで、上記本発明の個人情報管理装置において、上記個人情報格納部は、個人ごとの情報の中の各個別の情報それぞれがその各個人により複数のランクのうちのいずれかのランクに指定されることにより、各個人内で複数にランク付けされてなる個人情報が登録されたものであり、

上記開示手続格納部は、各個人により指定された、各個人内の各ランクに応じた情報開示手続が登録されたものであって、

上記開示手続実行部は、特定の個人の情報の開示依頼を受け、上記開示手続格納部に格納された、その特定の個人の、開示依頼を受けた情報のランクに応じた情報開示手続に合致した情報開示手続を実行するものであることが好ましい。

【０００８】

個人情報の中には、開示されてもさしたる支障のない個人情報や、ＪＩＳＱ　１５００１に規定されている、人種、民族、精神障害、信教等々の、極秘にされるべき機微の個人情報など、情報開示に関し様々なレベルの個人情報が存在する。

【０００９】

そこで、上記のように、各個人内で個人情報を複数のランクに分けておき、個人情報の開示にあたっては、開示しようとするように応じた情報開示手続に従って開示することにより、一層きめ細かに、個人情報の保護と開示のバランスをとることができる。

【００１０】

ここで、各ランクごとの情報開示手続は、各個人により各個人ごとに指定されたものであり、どのランクの情報であってもその個人の意図に反して開示されることが防止される。また、ここでは、各個別の個人情報のランクの指定も各個人に委ねられているため、各個別の個人情報についても各個人の考え方や環境に応じた保護が図られる。

【００１１】

また、上記本発明の個人情報管理装置において、上記開示手続格納部は、各個人により指定された、各個人ごとの平常時の情報開示手続に加え、各個人により指定された、各個人ごとの緊急時の情報開示手続が登録されたものであって、

上記開示手続実行部は、平常時と緊急時とを識別する情報を伴った、特定の個人の情報の開示依頼を受け、その開示依頼が平常時あるいは緊急時のいずれに属するかに応じて、開示手続格納部に格納された、その特定の個人の、それぞれ平常時の情報開示手続あるいは緊急時の情報開示手続に合致した情報開示手続を実行するものであることが好ましい。

【００１２】

緊急時、例えば本人が事故に遭遇して情報開示の意図を伝えることができないような状況においてまで平常時と同一の情報開示手続を要求するのは適当ではなく、平常時と緊急時とを分け、緊急時には、あらかじめ各個人により指定された、各個人の緊急時の情報開示手続に従うことが好ましいからである。

【００１３】

また、上記本発明の個人情報管理装置において、上記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、その個人への連絡手続が登録されたものであって、

上記開示手続実行部は、特定の個人の情報の開示依頼を受けて、その特定の個

人に、上記開示手続格納部に格納されたその特定の個人への連絡手続に合致した連絡手続で、個人情報の開示依頼があった旨通知して、通知を受けた個人からの情報開示の承認を受ける開示依頼通知部を備え、その開示依頼通知部により情報開示の承認を受けて、さらに情報開示手続を進めるものであることが好ましい。

【００１４】

ある個人の情報の開示依頼があった場合に、情報開示手続の一部に、その個人に連絡してその個人の情報の開示依頼があったことを通知し、情報開示について、その個人の承諾を受けるという手続を含ませることにより、その個人が知らない間に自分の情報が開示されるという事態を避けることができる。

【００１５】

さらに、上記本発明の個人情報管理装置において、上記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、その個人本人であることを認証する認証手続が登録されたものであって、

上記開示手続実行部は、特定の個人の情報の開示依頼を受けて、上記開示手続格納部に格納されたその特定の個人の認証手続に合致した認証手続でその特定の個人の認証を行なう認証部を備えたものであることが好ましい。

【００１６】

個人情報を開示する場合、その個人の許可を得るとともに、認定手続により、その許可した本人が正にその本人であることを確認することが好ましいが、その認証手続も、その個人があらかじめ指定しておいた認証手続に沿って進めることによりその個人の意思を反映させることができる。

【００１７】

ここで、上記のような、開示依頼通知部と認証部との双方を備えた場合、上記開示手続実行部は、開示依頼通知部により情報開示の承認を受けた後において、認証部により、開示手続格納部に格納された特定の個人の認証手続に合致した認証手続でその特定の個人の認証を行なうが好ましい。

【００１８】

さらに、上記本発明の個人情報管理装置において、上記開示手続格納部は、個人ごとに、その個人に代わって情報開示手続を進める権限が委譲された権限委譲

者の登録が自在なものであって、

上記開示手続実行部は、特定の個人の情報の開示依頼を受け、開示手続格納部にその特定の個人に代わって情報開示手続を進める権限が委譲された権限委譲者が登録されていた場合には、その特定の個人の情報を開示するための手続として、開示手続格納部に格納された、その権限委譲者の情報開示手続に合致した情報開示手続を実行するものであることが好ましい。

【００１９】

こうすることにより、例えば子供に対する親権者や、要介護人に対する介護者等が、本人に代わって、その本人の個人情報を保護しつつ、その本人の個人情報の開示手続を進めることができる。

【００２０】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

【００２１】

図１は、本発明の個人情報管理装置の一実施形態を含む個人情報管理・開示システムの一例を示す模式図である。

【００２２】

ここには、本発明の個人情報管理装置の一実施形態に相当する１台のサーバマシン１００と、代表的に２台のクライアントマシン２００，３００が示されており、それらは通信回線網５００に接続されている。

【００２３】

２台のクライアントマシン２００，３００のうちの１台のクライアントマシン２００は、情報提供者側のクライアントマシンであり、もう１台のクライアントマシン３００は、情報利用者側のクライアントマシンである。ここには情報提供者側のクライアントマシンと情報利用者側のクライアントマシンが１台ずつ示されているが、これらは代表的に示したものであり、通常は、多数台の情報提供者側のクライアントマシンおよび多数台の情報利用者側のクライアントマシンが通信回線網５００に接続されている。

【００２４】

情報提供者側のクライアントマシン２００には、携帯電話２１０が接続されている。すなわち、例えば、クライアントマシン２００に送られてきた電子メールが携帯電話２１０に転送されたり、また、携帯電話２１０はクライアントマシン２００を介してこのシステムにアクセス可能となっている。この図１では、携帯電話２１０は、矢印により、クライアントマシン２００に直接に接続されているかのように示されているが、この矢印はクライアントマシン２００と携帯電話２１０が上記の意味で接続されていることのみを示すものであって、実際には、それらは、図示しない無線通信回線を含む通信回線網５００を介して接続されている。

【００２５】

この図１に示すサーバマシン１００および２台のクライアントマシン２００，３００は、ＣＰＵ、主記憶装置、ハードディスク、通信用ボード等が内蔵された本体部１０１，２０１，３０１、本体部１０１，２０１，３０１からの指示により表示画面１０２ａ，２０２ａ，３０２ａ上に画像や文字列を表示する表示部１０２，２０２，３０２、サーバマシン１００および各クライアントマシン２００，３００にユーザの指示を入力するためのキーボード１０３，２０３，３０３、表示画面１０２ａ，２０２ａ，３０２ａ上の任意の位置を指定することにより、その指定時にその位置に表示されていたアイコン等に応じた指示を入力するマウス１０４．２０４，３０４を備えている。

【００２６】

また、サーバマシン１００およびクライアントマシン２００，３００の本体部１０１，２０１，３０１にはさらに、外観上、フロッピィディスク（ＦＤ）、ＣＤＲＯＭ（図１には図示せず：図２参照）が装填されるＦＤ装填口１０１ａ，２０１ａ，３０１ａ、ＣＤＲＯＭ装填口１０１ｂ，２０１ｂ，３０１ｂを有しており、それらの内部には、それらの装填口１０１ａ，２０１ａ，３０１ａ；１０１ｂ，２０１ｂ，３０１ｂから装填されたフロッピィディスクやＣＤＲＯＭをドライブしてアクセスする、フロッピィディスクドライブ、ＣＤＲＯＭドライブも内蔵されている。さらに、これらサーバマシン１００および各クライアントマシン２００，３００の本体部１０１，２０１，３０１は、通信回線網５００に接続さ

れている。

【００２７】

さらに各クライアントマシン２００，３００には、音声を入力するためのマイクロホン２０５，３０５、および指紋を読み取る指紋読取装置２０６，３０６が接続されている。

【００２８】

さらに、上述したように、情報提供者側のクライアントマシン２００には携帯電話２１０が接続されている。

【００２９】

図２は、図１に示すサーバマシンのハードウェア構成図である。クライアントマシンについては、マイクロホンと指紋読取装置が接続されていることを除き、サーバマシンと同様なハードウェア構成を有しており、ここでは、サーバマシンのハードウェア構成の図示および説明で代表させる。

【００３０】

ここには、中央演算処理装置（ＣＰＵ）１１１、ＲＡＭ１１２、ハードディスクコントローラ１１３、ＦＤドライブ１１４、ＣＤＲＯＭドライブ１１５、マウスコントローラ１１６、キーボードコントローラ１１７、ディスプレイコントローラ１１８、および通信用ボード１１９が備えられており、それらはバス１１０で相互に接続されている。

【００３１】

ＦＤドライブ１１４、ＣＤＲＯＭドライブ１１５は、図１を参照して説明したように、フロッピィディスク６１０、ＣＤＲＯＭ６２０が装填され、装填されたフロッピィディスク６１０、ＣＤＲＯＭ６２０をアクセスするものである。

【００３２】

また、ここには、ハードディスクコントローラ１１３によりアクセスされるハードディスク１２０、マウスコントローラ１１６により制御されるマウス１０４、キーボードコントローラ１１７により制御されるキーボード１０３、ディスプレイコントローラ１１８により制御される表示部１０２、および通信用ボード１１９を介して接続される通信回線網５００も示されている。

【００３３】

ＣＤＲＯＭ６２０には、図１に示すサーバマシン１００を、本発明の個人情報管理装置の一実施形態として動作させるための個人情報管理プログラムが記憶されており、ＣＤＲＯＭドライブ１１５により、そのＣＤＲＯＭ６２０から個人情報管理プログラムが読み込まれ、バス１１０を経由し、ハードディスクコントローラ１１３によりハードディスク１２０内に格納される。実際の実行にあたっては、そのハードディスク１２０内の個人情報管理プログラムはＲＡＭ１１２上にロードされ、ＣＰＵ１１１により実行される。

【００３４】

図３は、本発明の個人情報管理装置の一実施形態を表わす機能ブロック図である。この図３に示す個人情報管理装置は、図１，図２に示すサーバマシン１００のハードウェアと、ＣＤＲＯＭ６２０からインストールされた個人情報管理プログラムとの複合、及びその後の個人情報等の蓄積により構成されたものである。

【００３５】

この図３に示す個人情報管理装置７００は、個人情報格納部７１０と、開示手続格納部７２０と、開示手続実行部７３０とから構成され、開示手続実行部７３０は、さらに開示依頼通知部７３１と認証部７３２を備えている。

【００３６】

個人情報格納部７１０には、個人ごとの情報が登録されている。

【００３７】

図４は、個人情報格納部に登録された個人情報テーブルを示す図である。

【００３８】

ここには、１人分の個人情報の極く一部が示されており、そこには、住民基本番号、住所、氏名、生年月日、性別、介護等級、……等々、様々な個人情報が列記されている。

【００３９】

図３の開示手続格納部７２０には、各個人により指定された各個人ごとの情報開示手続が登録されている。

【００４０】

図５～図１０は、各個人ごとの情報開示手続を実行するのに必要な各種テーブルの例を示す図である。

【００４１】

具体的には図５，図６，……，図１０には、それぞれ、認証用データテーブル、情報開示手続テーブル、平常時認証テーブル、緊急時認証テーブル、通信順テーブル、および権限委譲テーブルが示されている。

【００４２】

図５に示す認証用データテーブルは、各個人について１つずつ作成されている。この認証用データテーブルには、その個人の認証に必要となる、例えばパスワード、指紋、声紋、ＤＮＡ、……等々のデータが登録されている。尚、この認証用データテーブルは個人情報の一種でもあり、これらのデータは、図４の個人情報テーブルに含まれていてもよいが、ここでは後の説明の都合上、個人情報テーブルとは別に認証用データテーブルを置いている。

【００４３】

また、図６に示す情報開示手続テーブルは、各個人の各開示レベルそれぞれについて１つずつ作成されている。この情報開示手続テーブルには、開示レベル、開示項目、および認証方法が登録されている。開示レベルは、本実施形態では、１～５のランクに分けられており、その数値が大きくなるほど秘密性が高いことを意味している。開示項目の欄には、その開示レベル（この図６に示す例では開示レベル１）に相当する個人情報の項目が列挙されている。また、認証方法の欄には、その開示レベルの個人情報を開示するための認証方法が登録されている。ただし、ここには、直接的には、その認証方法が登録された、図７の平常時認証テーブルを指し示すポインタが登録されている。

【００４４】

この図６に示す情報開示手続テーブルは、標準的な構成のガイダンスを受けつつも、その個人の考えで登録されたものである。すなわち、例えば開示レベル１に、どの個人情報を登録するか、あるいは、開示レベル１の個人情報を開示するための認証方法をどうするかは、その個人の判断に委ねられている。

【００４５】

図７に示す平常時認証テーブルは、図６の情報開示手続テーブルと同様、各個人の各開示レベルごとに作成されており、それぞれが各個人の各開示レベルごとの情報開示手続テーブル（図６参照）の認証方法の欄のポインタで指し示されている。各開示レベルごとの平常時認証テーブルには、その個人の、平常時の、各開示レベルごとの認証手続が登録されている。

【００４６】

この図７に示す例では、平常時には、パスワードと、指紋と、声紋の全てが一致した場合のみ、そのリンクされた情報開示手続テーブル（図６参照）に項目が列挙されている個人情報の開示を許可することを意味している。

【００４７】

図８に示す緊急時認証テーブルは、各個人につき１つずつ作成されており、そこには、その個人が意識不明に陥ったときなど、その個人が情報開示／非開示の意思をあらわすことができず、かつ、その個人の情報が緊急に必要となった場合の認証方法が登録されている。この図８に示す例では、緊急時には、その個人の指紋あるいはＤＮＡのいずれか１つが確認されることをもって、その個人の情報を開示することを示している。この図８の緊急時認証テーブルも、その個人の意思で登録されており、仮に、この緊急時認証テーブルが空欄であった場合、あるいは本人自身でないと認証が不可能な、例えばパスワードのみが登録されていた場合は、法律上規定された例外等の場合を除き、たとえその個人の生命が危機に晒された場合であっても情報は開示されない。緊急時の情報開示の依頼は、もともと救急指定病院の医師等、限られた者にのみ許可されており、本実施形態では、この緊急時認証テーブルに登録された認証方法に合致した場合、依頼に応じて全ての情報が開示される。ただし、緊急時であっても、例えば犯罪歴、門地等、緊急性に乏しくかつ秘密性の高い情報は非開示とするなど、開示される情報に制限を加えてもよい。

【００４８】

図９に示す通知順テーブルは、各個人ごとに作成されており、そこには、その個人に何かを通知するときの通知方法の順序が登録されている。この通知順テーブルも各個人が自分の意思で登録する。図９に示す例は、先ずは携帯電話に連絡

し、通じなかったときはそこに登録された別の電話にかけ、それでも通じなかったときは電子メールで連絡し、所定時間（例えば１５分間）経過しても返答がないときは代理人１に連絡をし、代理人１への連絡を試みても連絡できないときは代理人２に連絡することを意味している。代理人１、代理人２への連絡方法は、図９に示す通知順テーブルと同様な、その代理人１、代理人２の通知順テーブルに従うことになる。ただし、その代理人個人の通知順テーブルに、その代理人個人の、さらなる代理人が登録されていても、代理人個人の代理人への連絡は行なわれない。

【００４９】

図１０に示す権限委譲テーブルは、各個人のうちの必要な個人について作成される。

【００５０】

例えば、その個人が所定年齢以下の子供のときは、この権限委譲テーブルにはその子供の親権者が登録され、あるいは、その個人が要介護者であって介護等級が所定等級以上のときは、その要介護者を介護する介護人が登録される。

【００５１】

図３に戻って説明を続ける。

【００５２】

開示手続実行部７３０は、基本的には、通信回線網５００を経由した、特定の個人の情報の開示依頼を受け、開示手続格納部７２０に格納された、その特定の個人の情報開示手続に合致した情報開示手続を実行し、その情報開示手続が満足された場合に、個人情報格納部７１０に格納された個人情報の中から、その特定の個人の開示要求を受けた情報を抽出し、その抽出した情報を依頼元に向けて通信回線網５００に送信するものである。具体的には、開示手続格納部７２０に、個人ごとの情報開示手続の一部として、各個人により指定されたその個人への連絡手続と、各個人により指定されたその個人本人であることを認証する認証手続が登録されており、開示手続実行部７３０は、特定の個人の情報の開示依頼を受けて、基本的には先ず開示依頼通知部７３１により、その特定の個人に、開示手続格納部７２０に格納されたその特定の個人への連絡手続に合致した連絡手続で

、個人情報の開示依頼があった旨通知して、通知を受けた個人からの情報開示の承認を受ける。次に、開示手続実行部７３０は、今度は認証部７３２により、開示手続格納部７２０に格納されたその特定の個人の認証手続に合致した認証手続でその特定の個人の認証を行なう。ただし、その特定の個人本人ではなく、その代理人や保護者等に連絡し、その代理人や保護者等の認証を行なう場合もある。詳細は後述する。この認証手続が正しく終了すると、開示要求を受けた情報が抽出され要求元に向けて送信される。

【００５３】

以下、個人情報開示の手続きの一例について説明するが、ここでは、その説明のための１つの場面設定として、図１に示すクライアントマシン２００を自宅に備えた患者が、携帯電話２１０を持って、診察のために、クライアントマシン３００が設置された医院を訪れた場面を想定する。

【００５４】

図１１は、図２に示すサーバマシン１００における情報開示手続を示すフローチャートである。

【００５５】

図１のクライアントマシン３００が設置された医院の医師は、訪れてきた患者の病歴やアレルギー体質等を知るために、クライアントマシン３００を操作して、サーバマシン１００に対して、その患者のそれらに関する情報を送るよう要求する。

【００５６】

サーバマシン１００は、情報開示要求を受信すると（図１１ステップＳ１）、その情報開示要求が、この実施形態の対象である個人情報の開示要求であるか否かを判断し（ステップＳ２）、個人情報とは無関係の情報開示要求（例えば政府や公共機関の案内など）であったときは、その情報の性質に合った処理がなされる（ステップＳ３）。

【００５７】

ステップＳ２で、今回の情報開示要求が個人情報の開示要求である旨判定されると、次にその開示要求が緊急のものか否かが判定される。

【００５８】

ステップＳ４で平常時の情報開示要求である旨判定されると、ステップＳ５に進み、その個人情報の持ち主、すなわちここでは、医院を訪れた患者に向けて個人情報の開示要求があった旨通知され、その個人（患者）の、個人情報開示の同意が求められる。その開示に同意が得られないときは、非開示となり（ステップＳ６）、その旨開示要求元に通知される。ステップＳ５の詳細については後述する。

【００５９】

開示に対し同意があったときはステップＳ７に進み、平常時の認証手続が行なわれる。この平常時認証手続の詳細についても後述する。

【００６０】

また、ステップＳ４で緊急である旨判定されると緊急時の認証手続が行なわれる（ステップＳ８）。この緊急時認証手続についても後述する。

【００６１】

ステップＳ７あるいはステップＳ８の認証手続で正しく認証が行なわれると（ステップＳ９）、その個人（患者）の、要求された個人情報が、その要求元（クライアントマシン３００）に対し開示される（ステップＳ１０）。一方、認証に失敗すると非開示となり（ステップＳ６）、要求元に対しその旨通知される。

【００６２】

図１２は、図１１のステップＳ５に示す、個人情報開示要求通知および開示の同意を求める手続の詳細フローを示す図である。

【００６３】

ここではまず、情報開示要求を受けた情報の所有者である個人が他の個人の保護下にあるか否かが判定される（ステップＳ５１）。

【００６４】

ここでは、例えば情報開示要求を受けた情報の所有者である個人（患者）の個人情報テーブル（図４参照）が参照され、その個人（患者）が所定年齢以下の子供であったり、あるいは介護等級が高い重度障害者であったりしたときは、その個人の情報開示の責任はその個人の保護者等にあり、そのときは、その個人の権

限委譲テーブル（図１０参照）が参照されて、その個人の情報開示の権限の委譲を受けている保護者等に対し、その個人の情報の開示要求があった旨通知される（ステップＳ５７）。

【００６５】

そのような保護を必要としない通常の大人の場合は、その本人に対し、情報開示要求があった旨通知される（ステップＳ５２）。このときの本人への通知にあたっては、その本人の通知順テーブルが参照され、この図９に示す例では、まず携帯電話に情報開示要求があった旨通知される。携帯電話からの応答がないときは、前述のとおり、その通知順テーブルにしたがって次の手順による通知が試みられる。

【００６６】

ここでは、その通知を受ける個人である患者は自分の携帯電話を持参して医院を訪れており、自分の携帯電話が鳴り、自動音声により情報開示要求があった旨通知される。そこで、その携帯電話のボタン操作、あるいは声による応答により、その情報開示に対する同意、不同意の意思表明が行なわれる。

【００６７】

ここで、サーバマシン１００（図１参照）は、その本人から同意する旨通知を受けると、次のステップＳ７（図１１参照）の平常時認証手続きに進み、一方、同意しない旨通知を受けると、ステップＳ６（図１１参照）に進み、開示しない旨クライアントマシン３００に通知される。

【００６８】

仮に、図９に示す通知順テーブルに従って、携帯電話、別の電話、電子メールの順に本人への連絡を試みても応答がなかったときは、ステップＳ５４に進み、その通知順テーブルに代理人が登録されているか否かが判定され、代理人が登録されているときは、その代理人への通知が試みられる（ステップＳ５５）。代理人への通知は、その代理人によって登録される通知順テーブルに従って行なわれるが、前述したように、その代理人の通知順テーブルにその代理人の代理人が登録されていても、その代理人の代理人への通知は行なわれない。

【００６９】

本人の代理人への通知が試みられた結果、その代理人から情報開示許可の連絡が来たときはステップＳ７に進み、このときはその情報開示許可を行なった代理人に対する認証手続きが行なわれる。代理人から情報開示不許可の回答が来たとき、あるいは代理人から（複数の代理人がいるときはそれら複数の代理人のいずれからも）回答がなかったときは、ステップＳ６に進み、非開示となる。

【００７０】

ステップＳ５１でその個人が他の個人の保護下にある旨判定されてステップＳ５７に進むと、その個人を保護する立場にある保護者等に対して、その保護者等の通知順テーブルに従って通知が試みられる。このとき、その保護者等の通知順テーブルに代理人が登録されていても、その代理人への連絡は行なわれない。

【００７１】

その保護者等に通知した結果（ステップＳ５７）、その保護者等から情報開示許可の回答を受けたときはステップＳ７に進み、このときは、その保護者等に対して平常時認証手続が行なわれる。一方、その保護者等から開示不許可の回答を受けたとき、あるいはその保護者等から応答がなかったときは、ステップＳ６に進み、非開示となる。

【００７２】

図１３は、図１１のステップＳ７における平常時認証手続の詳細フローを示す図である。

【００７３】

ここでは、その情報開示要求を受けた本人（患者）の情報開示テーブル（図６参照）が参照され、開示要求を受けた情報がどの開示レベルに指定されているか確認される（ステップＳ７１）。

【００７４】

次いで、その個人（患者）の、その開示レベルに応じた平常時認証テーブル（図７参照）が参照される。ここで、その個人に代わり、代理人あるいは保護者等の認証手続を行なうときは、その開示レベルに応じた、その代理人あるいは保護者等の平常時認証テーブルが参照される。ここでは、その個人本人の認証手続を行なうものとして説明を続ける。

【００７５】

図７に示す例では、「パスワード」と「指紋」と「声紋」とにより認証を行なうことが登録されており、この場合、サーバマシン１００は、クライアントマシン３００に対して、そこに登録されているパスワード、指紋、声紋の入力を要求する。その医院を訪れている患者は、クライアントマシン３００のキーボードから自分のパスワードを入力し、かつ指紋読取装置３６０に自分の指を押し当てて指紋を読み取らせ、さらにマイクロホン３０５に向かって発声することにより声紋を入力する。すると、それらのパスワード、指紋、声紋は、図１のサーバマシン１００に送られ、サーバマシン１００では、その送られて来たパスワード、指紋、声紋を、その個人（患者）の認証用データテーブル（図５参照）に登録されているパスワード、指紋、声紋と比較し、一致するか否かが判定される。

【００７６】

クライアントマシン３００から送られて来たパスワード、指紋、声紋のすべてが本人のものであると判定されると、認証ＯＫとなり、いずれか１つでも本人のものではない、あるいは、不明である旨判定されると認証ＮＧとなる。図１１のステップＳ９では、その認証がＯＫかＮＧかが判定される。

【００７７】

図１４は、図１１の開示のステップ（ステップＳ１０）の詳細フローを示す図である。

【００７８】

ここでは、その個人（患者）の個人情報テーブル（図４参照）が参照されて、開示要求のあった情報が抽出される（ステップＳ１０１）。また、本実施形態では、開示要求のなかったいくつかの情報について、偽情報を発生させて、その個人情報テーブルから抽出された情報に付加される（ステップＳ１０２）。このようにして一部に偽情報を含む個人情報が、その要求元であるクライアントマシン３００に送信される（ステップＳ１０３）。

【００７９】

クライアントマシン３００は、自分がどの情報について開示要求を行なったか知っているため、受信した、偽情報を含む情報の中から正しい情報のみを抽出す

ることができる。この正しい情報と偽情報との区別をクライアントマシン３００の操作を行なった医師等の人間に委ねると思わぬミスを生じるおそれがあるため、クライアントマシン３００がどのような情報について開示要求を行なったかを記憶しておき、サーバマシン１００から受け取った情報の中から開示を要求した情報のみを抽出し、正しい情報のみを医師等に提示することが好ましい。このように一部に偽情報を含ませることにより、サーバマシン１００からクライアントマシン３００に送信される途中で悪意の第三者がその個人情報を盗んでも正しい情報と偽りの情報とが識別できず、個人情報が保護されることになる。

【００８０】

図１１のステップＳ８の緊急時認証手続が行なわれる場合の例としては、例えば患者が意識不明で医院に運び込まれた場合を挙げることができる。

【００８１】

その医院は救急医療を行なう医院としてあらかじめサーバマシン１００に登録されており、その医院の設置されているクライアントマシン３００に特別なパスワード等を入力して操作することにより、サーバマシン１００では、そのクライアントマシン３００からの情報開示要求が緊急性の高いものとして取り扱われる。

【００８２】

ステップＳ８では、このような場合の認証手続が行なわれるが、ここでは、その本人（患者）の緊急時認証テーブル（図８参照）が参照される。

【００８３】

この図８に示す例では、あらかじめその本人により指紋とＤＮＡとのいずれかで認証を行なうことが登録されており、サーバマシン１００は、クライアントマシン３００に対し、指紋あるいはＤＮＡのデータを送るよう要求する。クライアントマシン３００では、その運び込まれた患者の指紋を指紋読取装置３０６で採取してサーバマシン１００に送り、あるいは、例えば事故で指が切断されてしまっていて指紋が使えないときはＤＮＡ分析を行なってその結果をクライアントマシン３００に入力しサーバマシン１００に送信する。

【００８４】

サーバマシン１００では、その個人（患者）の認証用データテーブルを参照し、指紋が送られてきたときはその指紋が本人のものか否かが判定され、ＤＮＡの分析結果が送られてきたときはそのＤＮＡが本人のものか否かが判定される。この緊急時認証手続（ステップＳ８）では、その緊急時認証テーブル（図８参照）に格納されている項目のうちのいずれか１つでも本人のものと認定されると認証ＯＫとなる。

【００８５】

ステップＳ８の緊急時認証手続で認証ＯＫあるいは認証ＮＧとなった後の手続は、ステップＳ７の平常時認証手続で認証ＯＫあるいは認証ＮＧとなった後の手続と同様である。

【００８６】

なお、以上の説明では省略したが、図１に示すシステムにおける、サーバマシン１００と各クライアントマシン２００，３００との間の通信は暗号化された形式で行なわれ、受信した側で復号化される。それら暗号化，復号化の技術としては既存の技術が用いられる。

【００８７】

【発明の効果】

以上説明したように、本発明によれば、個人情報が有効に保護されるとともに、その有効利用が図られる。

【図面の簡単な説明】

【図１】

本発明の個人情報管理装置の一実施形態を含む個人情報管理・開示システムの一例を示す模式図である。

【図２】

図１に示すサーバマシンのハードウェア構成図である。

【図３】

本発明の個人情報管理装置の一実施形態を表わす機能ブロック図である。

【図４】

個人情報格納部に登録された個人情報テーブルを示す図である。

【図５】

認証用データテーブルの例を示す図である。

【図６】

情報開示手続テーブルの例を示す図である。

【図７】

平常時認証テーブルの例を示す図である。

【図８】

緊急時認証テーブルの例を示す図である。

【図９】

通知順テーブルの例を示す図である。

【図１０】

権限委譲テーブルの例を示す図である。

【図１１】

サーバマシンにおける情報開示手続を示すフローチャートである。

【図１２】

図１１のステップＳ５に示す、個人情報開示要求通知および開示の同意を求める手続の詳細フローを示す図である。

【図１３】

図１１のステップＳ７における平常時認証手続の詳細フローを示す図である。

【図１４】

図１１の開示のステップ（ステップＳ１０）の詳細フローを示す図である。

【符号の説明】

１００　サーバマシン

２００，３００　クライアントマシン

１０１，２０１，３０１　本体部

１０２，２０２，３０２　表示部

１０２ａ，２０２ａ，３０２ａ　表示画面

１０３，２０２，３０３　キーボード

１０４，２０４，３０４　マウス

２０５，３０５　マイクロホン

２０６，３０６　指紋読取装置

２１０　携帯電話

５００　通信回線網

７００　個人情報管理装置

７１０　個人情報格納部

７２０　開示手続格納部

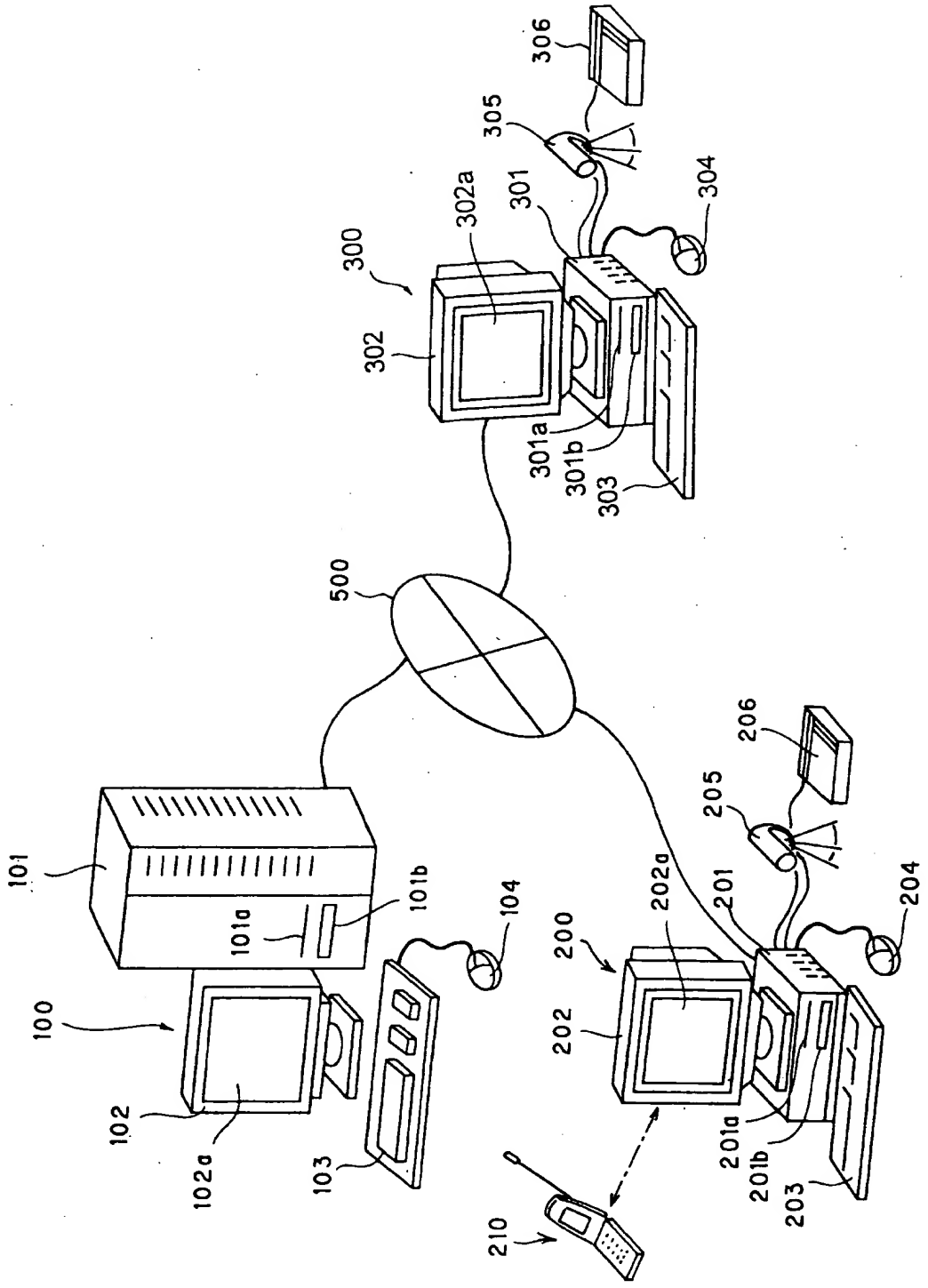
７３０　開示手続実行部

７３１　開示依頼通知部

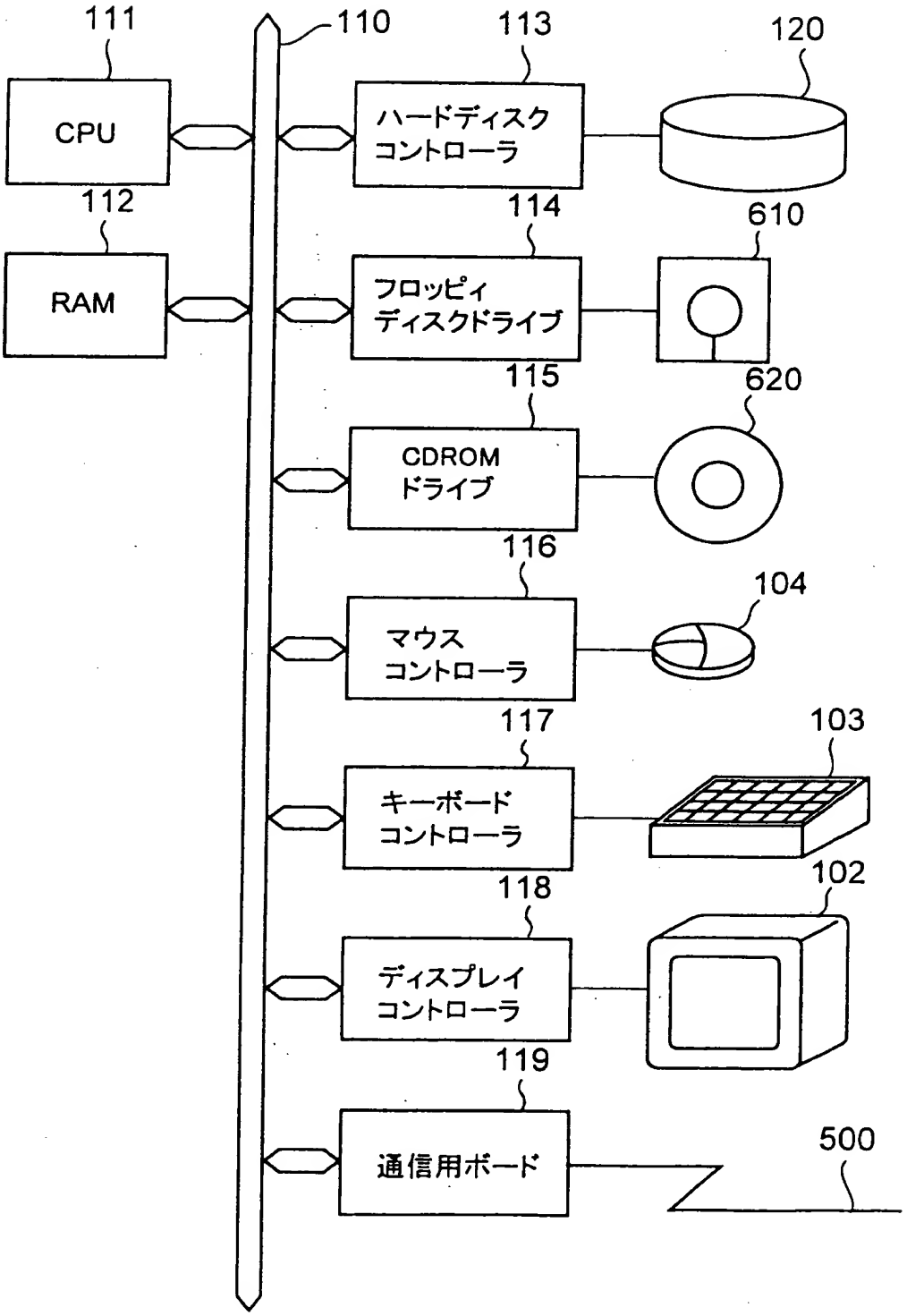
７３２　認証部

【書類名】　　図面

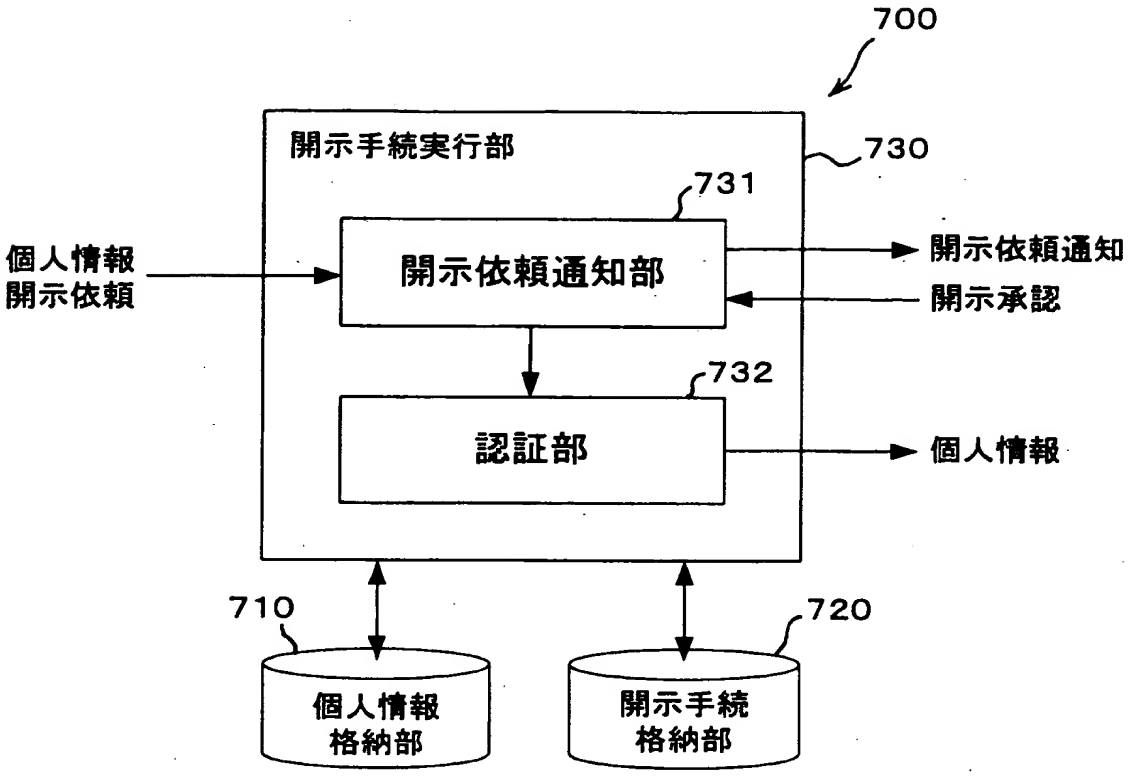
【図１】


306
305
304
302a
301
300
302
301a
301b
303
500
206
205
204
202a
201
200
202
201a
201b
203
101
101b
101a
104
100
102
102a
103
210

【図２】


111
110
113
120
CPU
ハードディスク
コントローラ
112
114
610
RAM
フロッピィ
ディスクドライブ
115
620
CDROM
ドライブ
116
104
マウス
コントローラ
117
103
キーボード
コントローラ
118
102
ディスプレイ
コントローラ
119
500
通信用ボード

【図３】



【図４】

個人情報テーブル

住民基本番号	住所	氏名	生年月日	性別	介護等級	

【図５】

認証用データテーブル

パスワード	指紋	声紋	DNA	

【図６】

情報開示手続テーブル

開示レベル	開示項目		認証方法
1	住所、氏名、------		(ポインタ)

【図７】

平常時認証テーブル

パスワード	指紋	声紋

【図８】

緊急時認証テーブル

指紋	DNA

【図９】

通知順テーブル

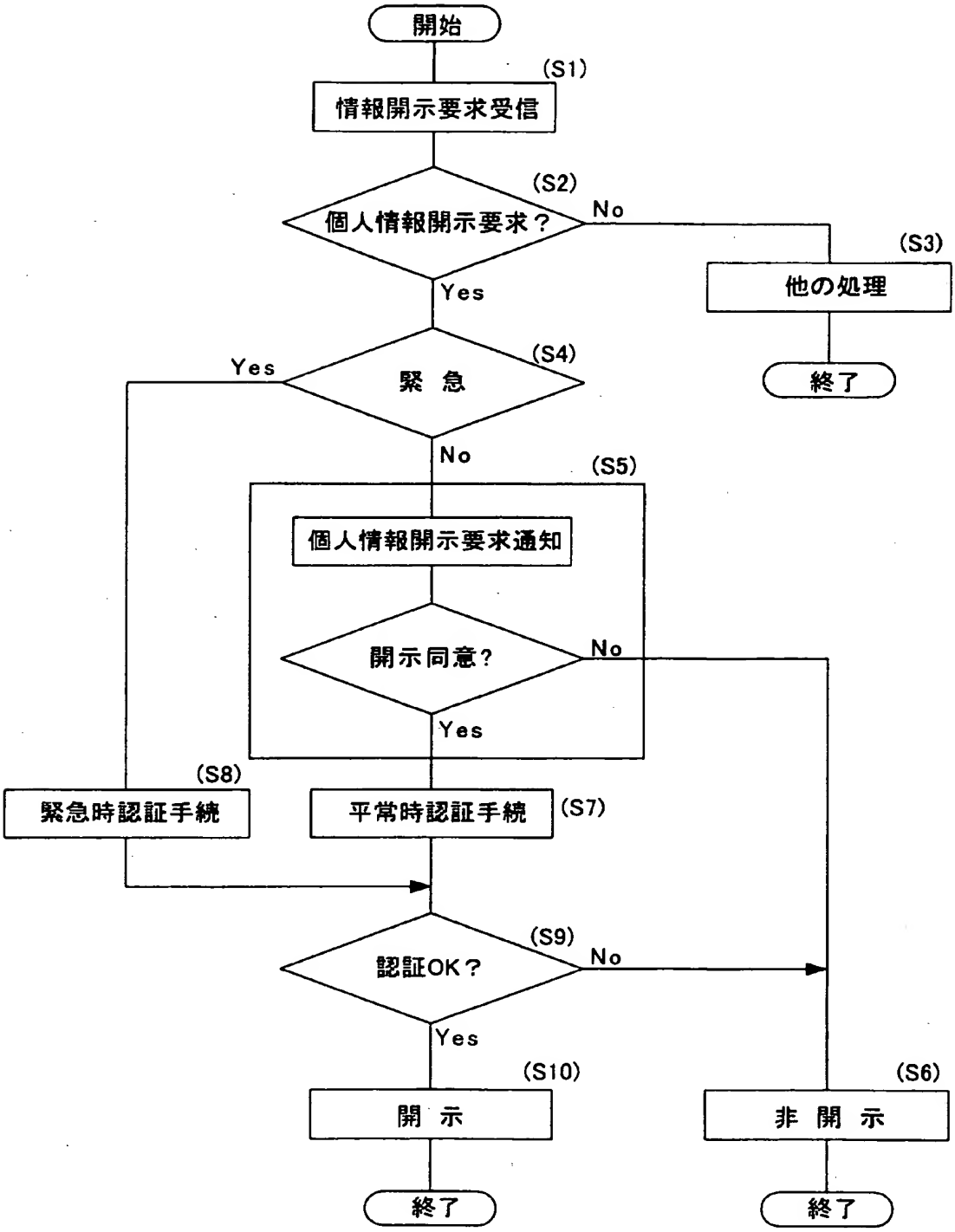
携帯	電話	メール	代理人1	代理人2		----------

【図１０】

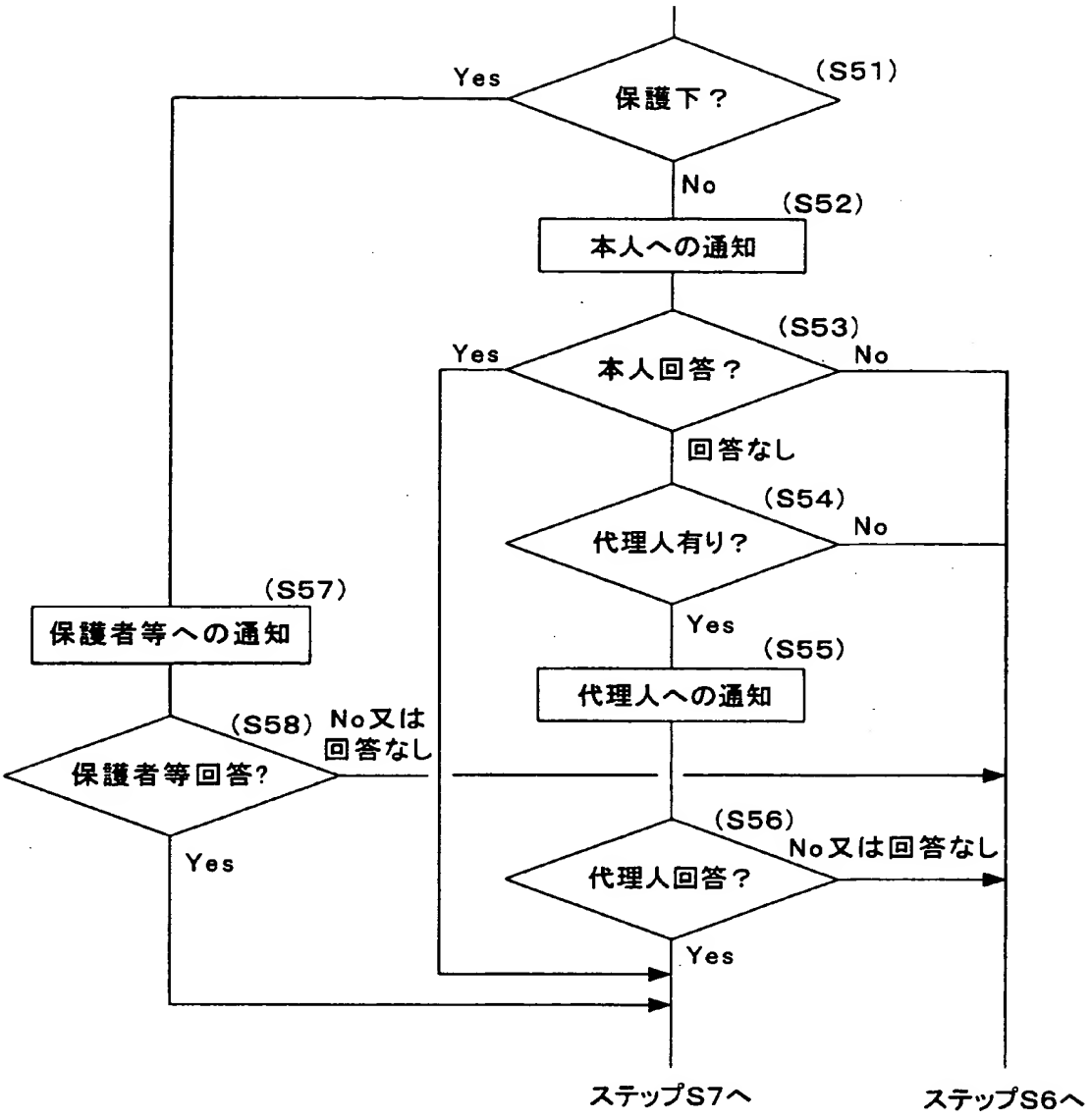
権限委譲テーブル

保護者	介護者		----------

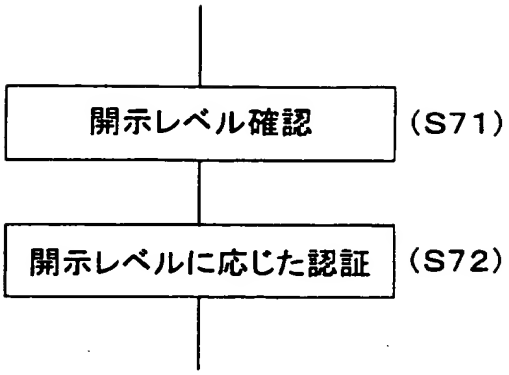
【図１１】


開始
(S1)
情報開示要求受信
(S2)
個人情報開示要求？
No
(S3)
他の処理
終了
Yes
(S4)
緊　急
Yes
No
(S5)
個人情報開示要求通知
開示同意？
No
Yes
(S8)
緊急時認証手続
平常時認証手続
(S7)
(S9)
認証OK？
No
Yes
(S10)
開　示
(S6)
非　開　示
終了
終了

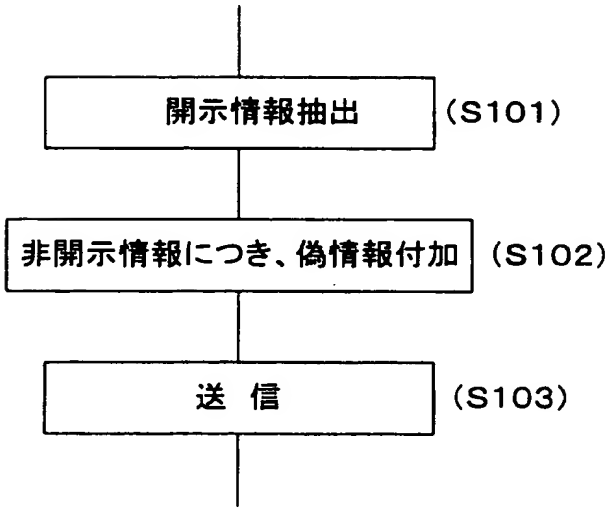
【図１２】


保護下？
(S51)
Yes
No
本人への通知
(S52)
本人回答？
(S53)
Yes
No
回答なし
代理人有り？
(S54)
No
Yes
代理人への通知
(S55)
保護者等への通知
(S57)
保護者等回答?
(S58)
No又は
回答なし
Yes
代理人回答？
(S56)
No又は回答なし
Yes
ステップS7へ
ステップS6へ

【図１３】


開示レベル確認
(S71)
開示レベルに応じた認証
(S72)

【図１４】


開示情報抽出
(S101)
非開示情報につき、偽情報付加
(S102)
送　信
(S103)

【書類名】　　要約書

【要約】

【課題】　本発明は、通信回線網に接続された、個人情報を管理する個人情報管理装置に関し、個人情報を有効に保護する。

【解決手段】個人ごとの情報が登録された個人情報格納部と、各個人により指定された各個人ごとの情報開示手続が登録されてなる開示手続格納部とを保護するとともに、特定の個人の情報の開示依頼を受けて、該特定の個人に、前記開示手続格納部に格納された該特定の個人への連絡手続に合致した連絡手続で、個人情報の開示依頼があった旨連絡して、連絡を受けた個人からの情報開示の承認を受ける開示依頼通知部と、前記開示手続格納部に格納された前記特定の個人の認証手続に合致した認証手続で該特定の個人の認証を行なう認証部とを有する開示手段実行部７３０を備えた。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社